REMARKS

Claims 18-38 stand rejected on prior art grounds. Additionally, claim 37 stands rejected under 35 U.S.C. §101. Claims 31-32 are herein cancelled. Thus, claims 18-30 and 33-38 are all the claims pending in the application. Applicants respectfully traverse these rejections based on the following discussion.

I. The 35 U.S.C. §101 Rejection

Claim 37 stands rejected under 35 U.S.C. §101. Specifically, the Office Action provides that the subject matter of a "computer program product" is not tangible. In order to overcome this rejection, claim 37 is amended herein to claim "a program storage device" rather than a "computer program product". In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw this rejection.

II. The Prior Art Rejections

Claims 18-30 and 33-38 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,279,113 issued to Vaidya on Aug. 21, 2001 (hereinafter referred to as Vaidya), in view of U.S. Patent No. 6,954,765 issued to Spiegel on Oct. 11, 2005 (hereinafter referred to as Spiegel). Applicants respectfully traverse these rejections because the cited prior art references do not teach each of the limitations of the claimed invention and further because the cited prior art references are not analogous prior art for the purpose of establishing obviousness under 35 U.S.C.§103.

More specifically, none of the following features which are amended herein into independent claims 18, 23, 30 and 37 are taught or suggested by the cited prior art references: (1) "receiving a packet of data addressed to an end-system in said network and comprising a fragment of a datagram"; (2) "determining if an entry is already contained in said normalization table for said datagram because of earlier received fragments"; (3) "if said entry is already contained in said normalization table, determining if any conflicts exist between said fragment and said earlier received fragments"; (4) "if a conflict exists, discarding said fragment"; and (5) "if said conflicts do not exist, simultaneously transferring said packet of said data to a network intrusion detection system and said end-system". Furthermore, none of the following additional features which are amended herein into independent claim 30 are taught or suggested by the cited prior art references: (1) "if said conflicts do not exist, determining if said fragment fits a bit mask"; (2) "if said fragment does not fit said bit mask, redirecting said fragment"; and (3) "if said fragment does fit said bit mask, simultaneously transferring said packet of said data to a network intrusion detection system and said end-system."

As discussed in the background section and paragraph [0078] of the present application, fragmentation of datagrams can result in ambiguities that can be exploited by an attacker in order to bypass the network intrusion detection system or to misuse the end-systems or the network intrusion system. These attacks can be based on the network's topology or on differences in handling procedures between the end-systems and the network intrusion detection system (see paragraph [0079]). Thus, the claimed invention is for a method for normalization of traffic data in order to eliminate these ambiguities. Specifically, a normalization table is dynamically established and maintained in a traffic normalizer (see paragraph [0089]). Then, referring to

Figure 7, the traffic normalizer receives a packet of data and determines if it is only a fragment of a datagram (see paragraph [0090]). If so, it is determined whether an entry is already contained in the normalization table for that datagram because of earlier received fragments (see paragraph [0090]). If there is no entry, a new entry is created for the datagram (see paragraph [0091]). If an entry has already been made in the table, it is updated and a determination is made as to whether or not any conflicts exists between the new fragment and any earlier received fragments (see paragraph [0093]). If such a conflict exists, then the fragment is discarded (see paragraph [0093]). If no conflicts exist, then a determination can be made regarding whether or not the fragment fits a bit mask. If the fragment does not fit the bit mask, the fragment can be redirected. If it does fit the bit mask, then the potential ambiguities are eliminated and the packet of data can be simultaneously transferred (i.e., forwarded) to both a network intrusion detection system and the end-system (see paragraph [0087]).

Per its Abstract, Vaidya discloses a network intrusion detection system that includes attack signature profiles. Each network object is assigned a set of attack signature profiles which is stored in memory. A monitoring device monitors network traffic for data packets addressed to the network objects. Upon detecting a data packet addressed to a specific one of the network objects, information is extracted from the data packet and used to identify the attack signature profiles corresponding to that network object. A virtual processor determines based on the profiles if the packet is associated with a known security violation. The cited portions of Vaidya (col. 3, lines 13-27 and col. 5, lines 33-39) describe the attack signature profiles that are maintained by the network intrusion detection system. Specifically, they indicate that an attack signature profile contains a description of the identifiable characteristics associated with a

particular network intrusion attempt (e.g., unauthorized data access, unauthorized data manipulations, etc.).

No where in the cited portions of Vaidya does it teach or suggest maintaining a normalization table with entries regarding datagrams, much less any of the other features set out above that are designed to eliminate ambiguities which would allow an attacker to bypass or misuse a network intrusion detection system (NIDS) or to misuse an end system. Rather than disclosing the limitations of the claimed invention, Vaidya simply discloses one example of a NIDS to which traffic data normalized according to the claimed invention can be forwarded. Furthermore, Vaidya and the claimed invention should not be considered analogous art for the purpose of determining obviousness under 35 U.S.C. §103 because they involve different fields of endeavor, namely, network intrusion detection and data transfer (i.e., normalization of traffic data being transferred over a network to a NIDS and an end-system) (see MPEP 2141.01(a)).

The other cited prior art reference, Spiegel, refers to a method for updating a file by making a backup copy of only those portions of a file that include changed data. Specifically, in its background section Spiegel indicates that reliable updating of files requires an entire backup copy of the file to be generated before updating the file. The backup copy restores the original if the file being updated becomes corrupted. However, making a backup copy of the whole file needlessly consumes storage space. To solve this problem, Spiegel provides a method for updating a stored file by only backing up those portions of the file that are to be changed. The method employs a fragmented file structure and sequence tables which connect the fragments together in the proper order (see col. 3, lines 45-55 and col. 4, lines 10-25). Backup copies are made for fragments of the file that are being updated (See col. 2, line 65-col. 3, line 5).

No where in the cited portions of Spiegel does it teach or suggest receiving a packet of data comprising a fragment of a datagram and maintaining a normalization table with entries regarding datagrams, much less any of the other features set out above that are designed to eliminate ambiguities which would allow an attacker to bypass or misuse a NIDS or to misuse an end-system. Furthermore, Spiegel and the claimed invention should not be considered analogous art for the purpose of determining obviousness under 35 U.S.C. §103 because they involve different fields of endeavor, namely, data storage and data transfer (i.e., normalization of traffic data being transferred over a network to a NIDS and an end-system) (see MPEP 2141.01(a)).

Therefore, amended independent claims 18, 23, 30 and 37 are patentable over Vaidya in view of Spiegel. Further, dependent claims 19-22, 24-29, 33-36 and 38 are similarly patentable, not only by virtue of their dependency from a patentable independent claim, but also by virtue of the additional features of the invention they define. Moreover, the Applicants note that all claims are properly supported in the specification and accompanying drawings, and no new matter is being added. In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw the rejections.

III. Formal Matters and Conclusion

With respect to the rejections to the claims, the claims have been amended, above, to overcome these rejections. In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw the rejections to the claims.

In view of the foregoing, Applicants submit that claims 18-30 and 33-38, all the claims presently pending in the application, are patentably distinct from the prior art of record and are in

condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary. Please charge any deficiencies and credit any overpayments to Attorney's Deposit Account Number 50-0510.

Respectfully submitted,

/Pamela M. Riley/

Dated: 2/6/07

Pamela M. Riley
Registration No. 40,146

Gibb I.P. Law Firm, LLC
2568-A Riva Road, Suite 304
Annapolis, MD 21401
Voice: (410) 573-0227
Fax: (301) 261-8825
Customer Number: 29154